(19) JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: 10334008 A

(43) Date of publication of application: 18.12.98

(51) Int. Cl G06F 13/00
G06F 12/14
G06F 15/00

(21) Application number: 09127079

(22) Date of filing: 16.05.97

(71) Applicant: INTERNATL BUSINESS MACH CORP <IBM>

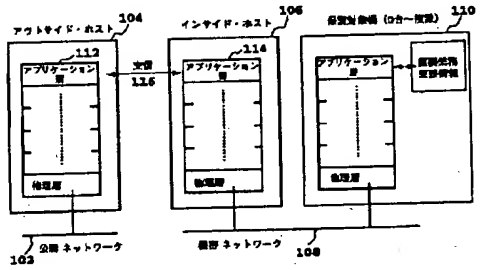
(72) Inventor: NEMOTO KAZUO

(54) NETWORK SECURITY SYSTEM

(57) Abstract:

PROBLEM TO BE SOLVED: To secure a high security in a system connected to a network.

SOLUTION: An outside host 104 is connected to an external network 102. A 1st connection program 112 for providing the security of the network 102 is stored in the host 104. The host 104 is connected to an inside host 106 through an exclusive transmission line 116. A 2nd connection program 114 is stored also in the host 106. The 1st and 2nd connection programs 12, 14 are respectively constituted of an application level program and a driver program for driving an exclusive transmission line. Communications can be attained only between the two connection programs 112, 114 and intrusion from the external can be prevented by executing communication only between two connection programs 112, 114. In addition, another part in the system can be prevented from being accessed.



(19)日本国特許庁（ＪＰ）　(12)**公開特許公報（Ａ）**　(11)特許出願公開番号

特開平10－334008

(43)公開日　平成10年(1998)12月18日

(51)Int.Cl.[6]		識別記号	FI		
Ｇ０６Ｆ	13/00	３５１	Ｇ０６Ｆ	13/00	３５１Ｍ
	12/14	３１０		12/14	３１０Ｎ
	15/00	３３０		15/00	３３０Ａ

審査請求　未請求　請求項の数５　ＯＬ　（全８頁）

(21)出願番号　特願平9－127079

(22)出願日　平成９年(1997)５月16日

(71)出願人　390009531
インターナショナル・ビジネス・マシーンズ・コーポレイション
INTERNATIONAL BUSINESS MASCHINES CORPORATION
アメリカ合衆国10504、ニューヨーク州　アーモンク　（番地なし）

(72)発明者　根本　和郎
神奈川県大和市下鶴間1623番地14　日本アイ・ビー・エム株式会社　大和事業所内

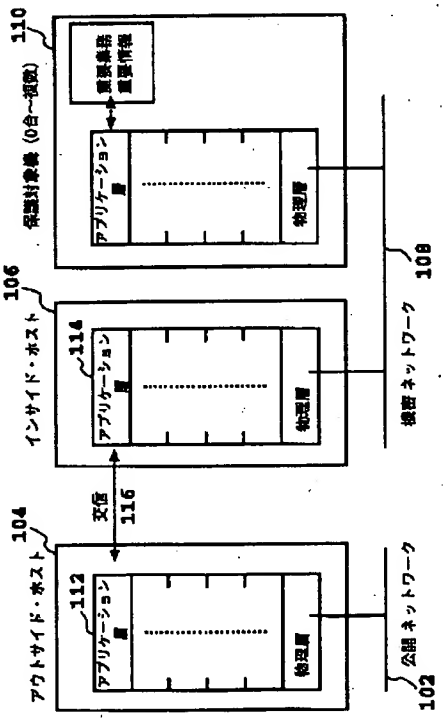
(74)代理人　弁理士　坂口　博　（外２名）

(54)【発明の名称】　ネットワーク・セキュリティ・システム

(57)【要約】

【課題】　ネットワークに接続されたシステムにおける高度のセキュリティの確保。

【解決手段】　外部からのネットワーク１０２に、アウトサイド・ホスト１０４が接続されている。このホスト１０４には、ネットワークのセキュリティを提供する第１接続プログラム１１２が実装されている。そして、このアウトサイド・ホストは、インサイド・ホスト１０６に専用の伝送路１１６を介して接続されている。このインサイド・ホストにも第２接続プログラム１１４が実装されている。この２つの第１と第２の接続プログラム１１２および１１４は、アプリケーション・レベルのプログラムおよび専用の通信路を駆動するドライバ・プログラムから構成されている。そして、２つの接続プログラム間のみで交信することで、外部からの侵入を防ぐことができる。また、システム内の他の部分にアクセスされることを防ぐことができる。



1

【特許請求の範囲】

【請求項１】　外部のネットワークと接続されているシステムにおいて、

外部ネットワークとの間でヘッダ付きパケットを送受信する第１のコンピュータと、

前記第１のコンピュータと専用の通信路で接続されている第２のコンピュータとを含み、

前記第１のコンピュータは、前記専用通信路を介して前記ヘッダ付きパケットからヘッダを落としたパケットを前記第２のコンピュータに送信し、前記第２のコンピュータから前記専用通信路を介した受け取ったパケットにヘッダを付加して前記外部ネットワークに対して送信することを特徴とするネットワーク・セキュリティ・システム。

【請求項２】　請求項１記載のネットワーク・セキュリティ・システムにおいて、前記通信路は、調歩式伝送により構成されていることを特徴とするネットワーク・セキュリティ・システム。

【請求項３】　請求項１または２記載のネットワーク・セキュリティ・システムにおいて、前記第２のコンピュータは、前記ヘッダを落としたパケットが予定のフォーマットであるか否かを判断することを特徴とするネットワーク・セキュリティ・システム。

【請求項４】　請求項１ないし３いずれか記載のネットワーク・セキュリティ・システムにおいて、前記第２のコンピュータは、第２のコンピュータと接続されているサーバーに対して、受信した前記パケットに含まれるデータを送信することを特徴とするネットワーク・セキュリティ・システム。

【請求項５】　請求項１ないし３いずれか記載のネットワーク・セキュリティ・システムにおいて、前記第２のコンピュータは受信した前記パケットに含まれるデータに対する処理を行い、処理結果を第１のコンピュータに送信することを特徴とするネットワーク・セキュリティ・システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、ネットワークに接続されたコンピュータ・システムにおいて、外部から機密を保持しなければならない内部システムに侵入されないようにしたネットワーク・セキュリティ・システムに関する。

【０００２】

【従来の技術】従来において、外部のネットワーク・システム例えばインターネットに接続されたコンピュータ・システムにおいて、外部からの侵入を防ぐシステムとしては、ファイアウォール・システムが知られている。このシステムは、ファイアウォールのプログラムを実装した要塞システムを設けることで、外部からの侵入を防ぐものである。このファイアウォールを二重に用いている２つの要塞ホストを使用したシステムも知られている。

2

【０００３】この２つの要塞ホストを使用したシステムを、図７および図８を用いて説明する。

【０００４】図７において、外部のネットワーク（インターネット）７０２に内部ネットワークを接続しているシステムを示している。インターネット７０２には、スクリーニング・ルーター７０４を介して内部ネットワークが接続されている。スクリーニング・ルーター７０４は、外部ネットワーク７０２から受信した内部ネットワーク向けのすべてのトラフィックを、要塞ホスト７０８の外側のネットワーク７０６に設定されている。また、スクリーニング・ルーター７０４は、トラフィックを要塞ホスト７０８に送る前にフィルタ・ルールを適用して、フィルタ・ルールをパスしたトラフィックのみが要塞ホスト７０８に送られる。

【０００５】アウトサイド・ネットワーク７０６は、非武装地帯（Demilitarized Zone：ＤＭＺ）を形成している。このアウトサイト・ネットワークは、ファイアウォールを搭載した要塞ホスト７０８によって守られていない。外部ネットワーク７０２からのトラフィックはアウトサイト要塞ホスト７０８を介して、プライベート・ネットワーク７１０に転送される。このプライベート・ネットワークは、ファイヤーウォールにより一応の機密性を保っているので、外部からアクセスするためのホストや、内部のあまり機密性を要しないホストをこの段階に設置することができる。

【０００６】より機密性の高いホストは、ファイアウォールを実装しているインサイド要塞ホスト７１２を介してプライベート・ネットワークに接続されているインサイド・ネットワーク７１４に接続する。このインサイド・ネットワークは、二重のファイアウォールにより守られているので、例えば電子署名のキー等の厳重な機密性を要するものを提供しているホストを接続する。

【０００７】

【発明が解決しようとする課題】このように、二重に守られているインサイド・ネットワークでは、二重であることにより強度はあげているが、二重化により特別な機能を提供はしておらず、通常のファイアウォールのプログラムを利用している限り限界がある。それは、ファイアウォールのプログラムが複雑であることや、アプリケーション・レベルで実行されていることに起因している。図７にその様子を示している。外部ネットワーク７０２からのトラフィックは、スクリーニング・ルーター７０４を介して、アウトサイド要塞ホスト７０８へと転送される。それから、インサイド要塞ホスト７１２を介してインサイド・ネットワーク７１４へと再度転送される。要塞ホスト７０８および要塞ホスト７１２には、ファイアウォールのプログラム７１６および７１８がアプリケーションの層で実装されており、この部分で外部か

らの侵入を防いでいる。

【０００８】そして、下位層の実装は、通常ＯＳと同等のレベルで行われている。この部分は、ユーザにとってはブラックボックスとなっている。そのため、この部分に外部からのアクセスに対して弱い部分があっても、通常のユーザは認知できず、気がついたときには、手遅れとなることも想定される。

【０００９】この様な例としては、例えば、ＯＳのバグ、ハードウェアの故障、各種ソフトウェアの設定ミス等がある。この様な原因で外部アクセスについての欠陥が生じた場合、オープン故障（動かなくなる）ならよいが、ショート故障（データが素通しで流れる）のときは重大なセキュリティ上の問題が生じる。

【００１０】このようなショート故障や、悪意によってファイアウォール・サーバーが汚染された場合には、例えばインターネットで用いられているプロトコルであるＴＣＰ／ＩＰのヘッダに含まれる宛先ＩＰアドレスやサービス・タイプ等は、フェイク可能であり、ドライバ・レベル（下位層）のチェックでは、不十分な場合もあった。

【００１１】一方、ＯＳに依存しないファイアウォールを開発することは、ＯＳレベルのコーディングを必要とし、不可能ではないにしても多大な労力および費用を要する。

【００１２】本発明は、このようなファイアウオールの本質的な部分の欠点を有さず、セキュリティの高いネットワーク・セキュリティ・システムを提供することを目的としている。

【００１３】

【課題を解決するための手段】上記目的を達成するために、本発明は、外部のネットワークと接続されているシステムにおいて、外部ネットワークとの間でヘッダ付きパケットを送受信する第１のコンピュータと、前記第１のコンピュータと専用の通信路で接続されている第２のコンピュータとを含み、前記第１のコンピュータは、前記専用通信路を介して前記ヘッダ付きパケットからヘッダを落としたパケットを前記第２のコンピュータに送信し、前記第２のコンピュータから前記専用通信路を介した受け取ったパケットにヘッダを付加して前記外部ネットワークに対して送信することを特徴とするネットワーク・セキュリティ・システムである。

【００１４】また、前記通信路は、調歩式伝送により構成することができる。

【００１５】前記第２のコンピュータは、前記ヘッダを落としたパケットが予定のフォーマットであるか否かを判断している。

【００１６】前記第２のコンピュータは、第２のコンピュータと接続されているサーバーに対して、受信した前記パケットに含まれるデータを送信することができる。

【００１７】前記第２のコンピュータは、受信した前記

パケットに含まれるデータに対する処理を行い、処理結果を第１のコンピュータに送信してもよい。

【００１８】このように、本発明の構成によれば、簡単な構成でセキュリティ強度の高いシステムを構築することができる。

【００１９】

【発明の実施の形態】本発明の実施形態を、図面を参照して詳細に説明する。

【００２０】図１は、本発明の実施の形態を説明するための図である。

【００２１】図１において、外部からのアクセスが容易なネットワーク（公開ネットワーク）１０２に、アウトサイド・ホスト１０４が接続されている。このホスト１０４には、本発明のネットワークのセキュリティを提供する第１接続プログラム１１２が実装されている。そして、このアウトサイド・ホストは、インサイド・ホスト１０６に専用の伝送路１１６を介して接続されている。このインサイド・ホストにも第２接続プログラム１１４が実装されている。この２つの第１と第２の接続プログラム１１２および１１４は、アプリケーション・レベルのプログラムおよび専用の通信路を駆動するドライバ・プログラムから構成されている。そして、２つの接続プログラムが通信路を占有するかたちで交信することで、外部からの侵入を防ぐことができる（通常のネットワークにおいては、占有されておらず、多重に使用されている）。また、システム内の他の部分にアクセスされることを防ぐことができる。この第１接続プログラム１１２および第２接続プログラム１１４については、後で詳しく説明する。

【００２２】インサイド・ホストはセキュリティが確保されているので、これに接続されている内部のネットワーク１０８は、機密ネットワークである。機密ネットワーク１０８には、外部からの侵入を保護すべき対象である重要な業務を行っており、重要な情報を有しているホスト１１０が接続されている。なお、保護対象機１１０は、接続プログラム１０６を実装しているインサイド・ホストで兼ねることもできる。この場合は、内部でのネットワーク接続された保護対象のホストがなくてもよい。

【００２３】さて、接続プログラム１１２および１１４について、図２を用いてさらに具体的に説明する。図２は、双方向のシリアル・ポートで接続し、調歩式伝送で交信している例を示している。図２において、アウトサイド・ホスト１０４とインサイド・ホストとの間を、ポート２０２およびポート２０４で接続している。このシリアル・ポート２０２およびポート２０４は２つの接続プログラムに専用となっており、この接続プログラムに含まれるこのポート専用のシリアル・ポート・デバイス・ドライバにより物理的にアクセスされる。このように外部から専用に接続し、しかも、機密ネットワーク１０

８を介して接続される外部からのアクセス対象である認証サーバー１１０等の保護対象のホストには、接続プログラムによりチェックを十分におこなってからアクセスすることが可能であるので、十分なセキュリティを確保することができる。

【００２４】この専用のシリアル・ポートにアクセスするためのシリアル・ポート・デバイス・ドライバは、簡単な構成なので自作しても、標準のドライバをテストして使用してもよい。

【００２５】従って、この接続はシステム外部からはアクセスすることができず、アウトサイド・ホストの特権ユーザであっても操作できない。また、専用のデバイス・ドライバを使用しているので、従来のファイアウオールを用いた場合と異なり、ＯＳ等のバグによるアクセスの穴がない。そして、この専用の接続プログラムや専用のポートや接続線が壊れるときは、２ヶ所に分散しているため、必ず動かなくなる方向である。

【００２６】また、外部からアクセスされる特定のサーバー例えば暗号を解読用のキーを発行する認証サーバー１１０のみにアクセスするための接続にのみこのポートによる接続を用いると、宛先情報が必要なく、その上、その認証サーバー１１０へのアクセス独特のチェックができ、より機密性が高まる。

【００２７】アウトサイド・ホストに実装されている第１接続プログラムは、例えば、上述のように、認証サーバーのみに使用している場合は、宛先（認証サーバー）が決まっており、輻輳制御が必要ない（他へのアクセスがないため）ので、データのみを必要最小限の制御情報（例えば、パリティビット等）を付与して送ればよい。また、この様に認証サーバー専用である場合は、交信するデータ量の少ないのでデータ転送速度もそれほど速い必要はない。

【００２８】この第１と第２の接続プログラムの動作について、図３および図４を用いて詳しく説明する。図３および図４では、暗号解読用のキーを発行している認証サーバー１１０専用に交信を行う場合で説明している。

【００２９】図３には、第１と第２の接続プログラムをアウトサイド・ホスト１０４とインサイド・ホスト１０６に実装した場合の構成が示されている。アウトサイド・ホスト１０４は、ユーザ・インタフェース機３０４に接続されている。ユーザ・インタフェース機３０４は、外部ネットワーク３０２に接続されており、外部からのアクセス者に対してホームページ等のユーザ・インタフェースを提供している。

【００３０】第１および第２の接続プログラムにはそれぞれ、送信側としてＡ－クライアント(A-client)とＣ－クライアント(C-client)を有し、受信側としてＢ－サーバー(B-server)とＤ－サーバー(D-server)を有している。

【００３１】アウトサイド・コンピュータ１０４のＡ－クライアントは、外部ネットワークと接続されているユーザ・インタフェース機３０４から送られてきた、例えばＴＣＰ／ＩＰプロトコルのヘッダを有しているパケットを受信する。次に、Ａ－クライアントは、パケットからヘッダを取り除いて必要なデータのみを調歩式データに変換し、シリアルポートを介してインサイド・ホスト１０６のＢ－サーバーに送る。Ｂ－サーバーは、認証サーバーのクライアント側（認証クライアント）として、認証サーバー１１０上のキーを管理しているプログラムである認証サーバー１１０にデータを送信する。

【００３２】認証サーバー１１０では、それが正当なキー発行要求であるならば、暗号解読用のキーを発行して、そのキー・データを認証クライアントであるインサイド・ホスト１０６に送る。受信した第２接続プログラムのＣ－クライアントは、アウトサイド・ホスト１０４のＤ－サーバーに調歩式データとしてキー・データをシリアルポートを介して送る。受信したＤ－サーバーは、プロトコルで必要なヘッダをまた付与して、ユーザ・インタフェース機３０４にキー・データを送る。なお、インサイド・ホスト１０６と認証サーバー１１０との間は、通常の通信で送られており、プロトコル上ヘッダが必要なら、インサイド・ホスト１０６内のＢ－サーバーが付与し、また、Ｄ－サーバーがそのヘッダを取り除いている。

【００３３】第１および第２接続プログラムの処理について、データの流れを中心に図４を用いてさらに詳細に説明する。

【００３４】図４において、具体的には、試用プログラムを使用したユーザーが、試用後に正式版であるプログラムを使うために、暗合化されたいる製品を、ＣＤ－ＲＯＭやテープ等から解読してインストールするためのキーをインターネット経由で得ることを想定している。

【００３５】インターネットからアクセスしたユーザは、ユーザ・インタフェース機３０４における解読キーを得るために、WWWのページにアクセスして画面の指示によりユーザＩＤ等を入力する。これはＲＥＱデータとして、ユーザ・インタフェース機３０４からアウトサイド・ホスト１０４に送られる。ＲＥＱデータの形式は例えば、図４（ｂ）に示す形式である。アウトサイド・ホストの第１接続プログラムは、ＲＥＱデータを受け取ると送られたパケットからヘッダを取り除いて、自分自身のキューに入れる。第１接続プログラムは、ＲＥＱデータをキューから受信の順番に、シリアル・ポートを介してインサイド・ホスト１０６の第２接続プログラムに送る。そして、キューの中の送ったＲＥＱデータに対して、キー作成中のフラグをたてる。

【００３６】送られてきたＲＥＱデータは、第２接続プログラムにおいて、データのフィールド検査を行う。これは図４（ｂ）において、ユーザＩＤ、取引ＩＤ、商品ＩＤの各々が決められた属性（例えば、数字等の文字種

や桁数）であるかの形式に関するチェックする。そして、正しい場合は自分自身のキューに入れる。正しくない場合はその旨第１接続プログラムにシリアル・ポートを介して伝える。

【００３７】インサイド・ホスト１０６の第２接続プログラムは、形式的に正しいＲＥＱデータを認証サーバー１１０に送るとともに、キー作成中のフラグをたてる。

【００３８】認証サーバー１１０は、送られてきたＲＥＱデータを検証し、その結果、確認がとれた場合は、キーを発行して、インサイド・ホスト１０６に発行したキーのデータを送る。検証の結果、キーが発行できない場合はその旨返送する。

【００３９】インサイド・ホスト１０６の第２接続プログラムでは、キー・データが送られてきたら、対応するフラグをたてたＲＥＱデータを消去する。送られてきたキー・データをシリアル・ポートを介してアウトサイド・ホスト１０４に送る。一定時間待って、送ったＲＥＱデータに対する応答がない場合には、そのＲＥＱデータを認証サーバー１１０に再送する。

【００４０】アウトサイド・ホスト１０４の第１接続プログラムは、キー・データをシリアル・ポートを介して第２接続プログラムから受け取ると、対応するＲＥＱデータを消去して、キー・データを必要なヘッダを付与してユーザ・インタフェース機３０４に送る。

【００４１】このように、アウトサイド・ホスト１０４とインサイド・ホスト１０６との間では、不必要なネゴシエーションは行っていない。これは、ネゴシエーションを行うことにより、この間のインタフェースのプロトコルが複雑になり、セキュリティ強度が下がるからである。

【００４２】なお、上記の実施形態において、データのチェックをインサイド・ホスト上の第２接続プログラムにおいて行ったが、第１接続プログラムで行うこともできる。

【００４３】インサイド・ホスト１０６は、認証サーバー１１０と兼用できる。この場合は、インサイド・ホスト１０６に認証サーバー１１０のためのプログラムを実装すればよい。インサイド・ホスト上の第２接続プログラムは、受信したデータを認証サーバー１１０に転送するのではなく、自機の認証サーバー・プログラムに送る。

【００４４】また、アウトサイド・ホストとユーザ・インタフェース機も兼用することができる。

【００４５】上述の図２～図４の説明においては、認証サーバーが１つのみの場合を説明したが、図５に示すように、認証サーバーを２つ以上用いることも可能である。この場合は、第２接続プログラムにおいて、例えば商品ＩＤによりＲＥＱデータの送り先を指定する必要がある。

【００４６】また、上記で説明したような接続形態を用

いて、図６に示すように、プロトコル層の中間で送受信する様な構成とすることもできる。このような構成とすると、プロトコルの解釈を２つのホスト機６０２および６０４で行うことができるので、セキュリティ強度を高めることが可能となる。このような場合の応用としてはルータ等がある。

【００４７】上記のプログラムでその機能を実行している部分に関して、それを記録媒体上に格納し、それをコンピュータ・システムで読み出すことにより、本発明を実施することもできる。この記録媒体には、フロッピー・ディスク、ＣＤ－ＲＯＭ、磁気テープ、ＲＯＭカセット等がある。

【００４８】

【発明の効果】上記の説明のように、本発明の構成を使用すると、外部とネットワークで接続されたシステムにおいて、簡単な構成でセキュリティ強度の高いシステムを構築することができる。

【図面の簡単な説明】

【図１】本発明の実施形態を示す図である。

【図２】本発明の実施形態を示すブロック図である。

【図３】本発明の詳しい実施形態を示すブロック図である。

【図４】本発明の実施形態のデータの流れを示すブロック図である。

【図５】本発明の詳しい実施形態を示すブロック図である。

【図６】本発明の詳しい実施形態を示すブロック図である。

【図７】従来のセキュリティ・システムを示す図である。

【図８】従来のセキュリティ・システムを示す図である。

【符号の説明】

１０２　公開ネットワーク
１０４　アウトサイド・ホスト
１０６　インサイド・ホスト
１０８　機密ネットワーク
１１０　保護対象機
１１２　第１接続プログラム
１１４　第２接続プログラム
１１６　伝送路
３０２　公開ネットワーク
３０４　ユーザ・インタフェース機
６０２　外側コンピュータ
６０４　内側コンピュータ
７０２　インターネット
７０４　スクリーニング・ルーター
７０６　アウトサイドＤＭＺネットワーク
７０８　アウトサイド要塞ホスト
７１０　インサイドＤＭＺネットワーク（プライベート

9

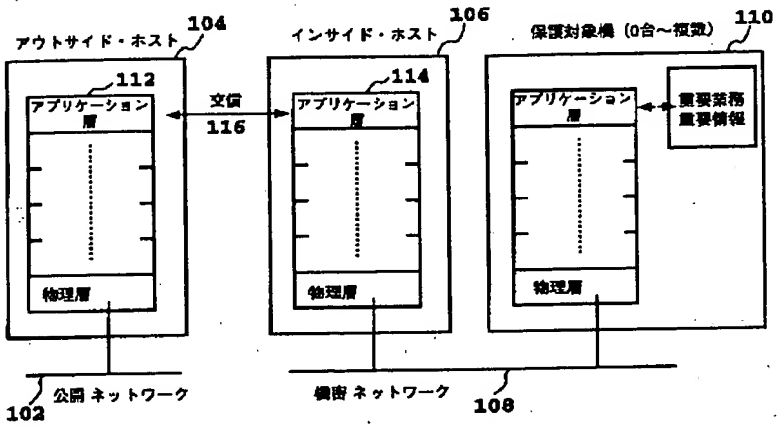
・ネットワーク）

７１２　インサイド要塞ホスト

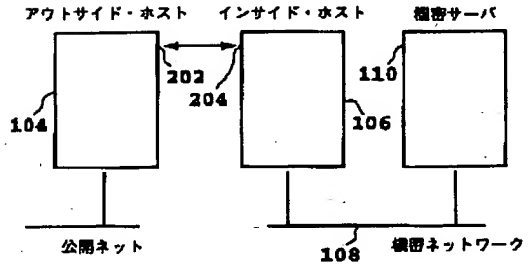
10

７１４　インサイド・ネットワーク

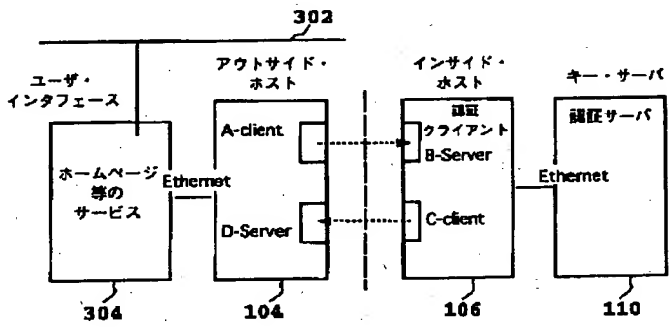
【図１】



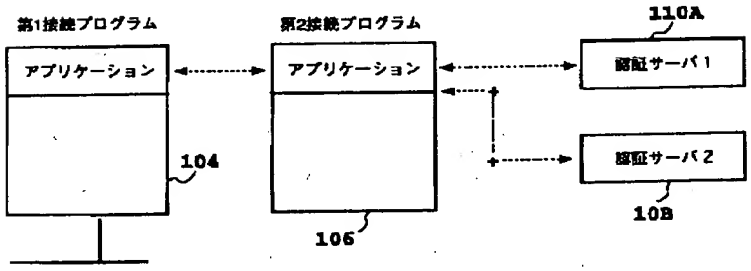
【図２】



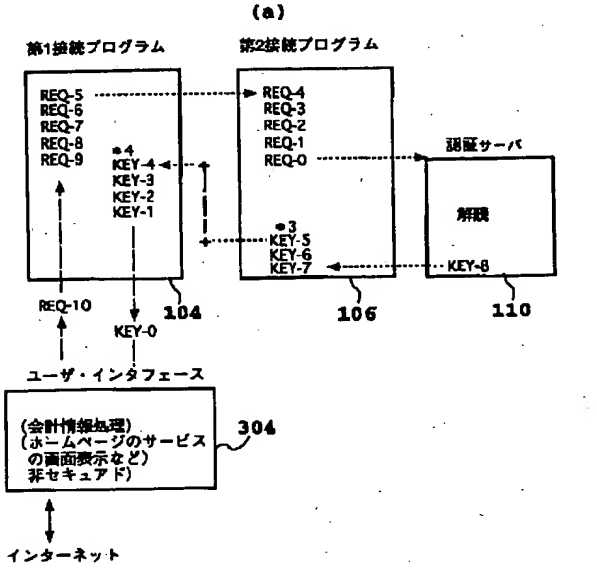
【図３】



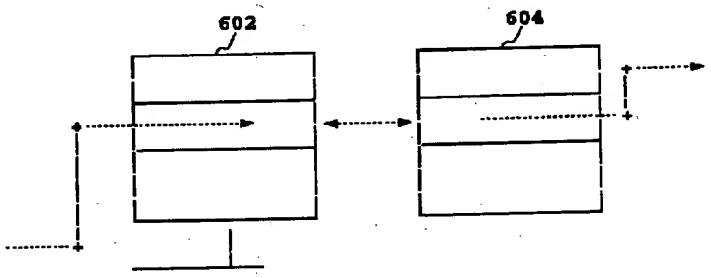
【図５】



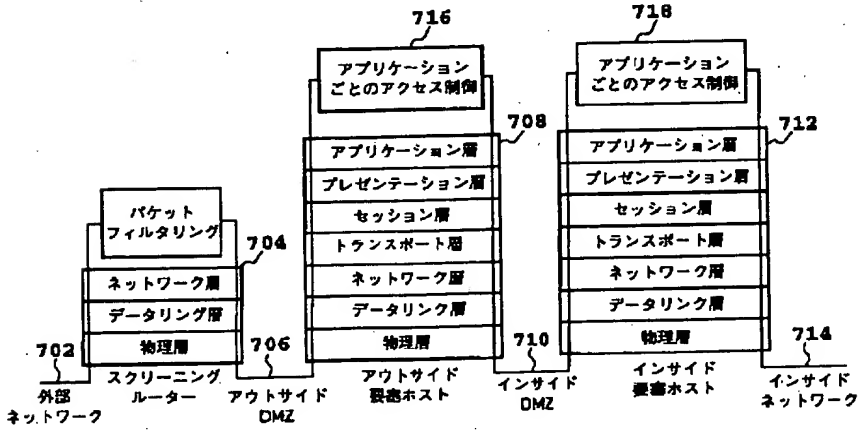
【図４】


(a)
第1接続プログラム
第2接続プログラム
REQ-5
REQ-6
REQ-7
REQ-8
REQ-9
●4
KEY-4
KEY-3
KEY-2
KEY-1
REQ-4
REQ-3
REQ-2
REQ-1
REQ-0
●3
KEY-5
KEY-6
KEY-7
認証サーバ
解読
KEY-8
REQ-10
KEY-0
104
106
110
ユーザ・インタフェース
(会計情報処理)
(ホームページのサービス
の画面表示など)
非セキュアド)
304
インターネット
(b)
REQデータ例
USER ID
取引 ID
商品 ID

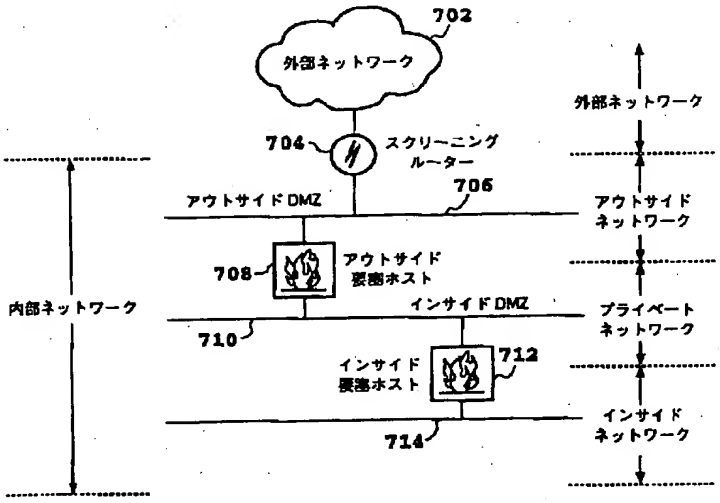
【図６】


602
604

【図８】


716
718
アプリケーション
ごとのアクセス制御
アプリケーション
ごとのアクセス制御
708
712
アプリケーション層
プレゼンテーション層
セッション層
トランスポート層
ネットワーク層
データリンク層
物理層
パケット
フィルタリング
704
ネットワーク層
データリング層
物理層
702
706
710
714
外部
ネットワーク
スクリーニング
ルーター
アウトサイド
DMZ
アウトサイド
要塞ホスト
インサイド
DMZ
インサイド
要塞ホスト
インサイド
ネットワーク

【図７】


702
外部ネットワーク
704
スクリーニング
ルーター
706
アウトサイドDMZ
708
アウトサイド
要塞ホスト
インサイドDMZ
710
712
インサイド
要塞ホスト
714
内部ネットワーク
外部ネットワーク
アウトサイド
ネットワーク
プライベート
ネットワーク
インサイド
ネットワーク